EPIF response to EDPB consultation on the interplay of the Second Payment Services Directive (PSD2) and the GDPR

September 2020

ABOUT EPIF (EUROPEAN PAYMENT INSTITUTIONS FEDERATION)

EPIF, founded in 2011, represents the interests of the non-bank payment sector at the European level. We currently have over 190 authorised payment institutions and other non-bank payment providers as our members offering services in every part of Europe. **EPIF** thus represents roughly one third of all authorized Payment Institutions ("PI") in Europe. All of our members operate online. Our diverse membership includes a broad range of business models, including:

- Three-party Card Network Schemes
- E-Money Providers
- E-Payment Service Providers and Gateways
- Money Transfer Operators
- Acquirers
- Digital Wallets
- FX Payment Providers and Operators
- Payment Processing Services
- Card Issuers
- Independent Card Processors
- Third Party Providers
- Payment Collectors

EPIF seeks to represent the voice of the PI industry and the non-bank payment sector with EU institutions, policy-makers and stakeholders. We aim to play a constructive role in shaping and developing market conditions for payments in a modern and constantly evolving environment. It is our desire to promote a single EU payments market via the removal of excessive regulatory obstacles.

We wish to be seen as a provider for efficient payments in that single market and it is our aim to increase payment product diversification and innovation tailored to the needs of payment users (e.g. via mobile and internet).

EPIF welcomes the EDPB guidelines intended to provide more clarity on the interplay of the Second Payment Services Directive (PSD2) and the GDPR and appreciates the opportunity to provide comments on the consultation.

Summary of comments on the Guidelines

- EPIF believes that the Guidelines interpret Article 66 and 67 unnecessarily strict with regard to the processing of personal data that PISPs and AISPs can undertake risking unwanted consequences for PISPs and AISPs effectively limiting their ability to provide service to the benefit of consumers.
- The Guidelines can be made more explicit with regards to the interpretation of explicit consent under Article 94 explicitly allowing for room for interpretation/manoeuvre depending on the specific payment services provided and the relevant payment service provider.

Services under PSD

It is suggested to remove from the guidelines the following statement in paragraph 8: ***"Services that entail creditworthiness assessments of the PSU or audit services performed on the basis of the collection of information via an account information service fall outside of the scope of the PSD2 and therefore fall under the GDPR".*** The PSD2 itself does not exclude those particular processing purposes from the definition of payment services (annex 1), so it should be the laws and guidelines implementing the PSD2 at a national level the ones determining if that example should be considered a payment service or not. In this regard some current national guidance on the scope of the PSD2 already recognizes Income analysis (including affordability assessment; credit rating assessments; and credit worthiness assessments) as activities included in the definition of services provided by an AISP.

Article 66 and 67 - explicit consent and further processing

In terms of specific comments, EPIF disagrees with the statements in paragraph 22 that Article 66 and 67 PSD2, from a GDPR perspective, considerably restrict the possibilities for processing for other purposes than as explicitly consented to by the user. As with any other processing of personal data, including for the processing of payment services more generally, a data controller needs to comply with GDPR and among others the basic principles (Article 5), legal basis (Article 6) and providing information (Article 13) in a transparent way (Article 12).

However, in line with payment services more general, as long as GDPR is complied with, processing of personal data is per default allowed, this includes also processing that is based on another legal basis than consent. The restriction imposed by PSD2 in Article 66 and 67 should rather be understood as limitations from a PSD2 regulatory perspective entailing that a PISP/AISP cannot use information pertaining to the user's payment accounts to initiate an new payment order unless the user has explicitly consented to the new payment order.

EPIF is concerned that the proposed interpretation of Article 66 and 67 in the Guidelines, and the conclusion that any other processing than providing the payment service that is requested is (typically)

not allowed, will result in unintended consequences. For example, PISPs only provide their payment initiation payment services upon the request of the user (i.e. with the user's explicit consent) as the user is actively choosing to pay with the PISP and is proceeding through their iframe by choosing his/her bank, bank account to pay from as well as authenticating the payment. In other words, is the payment service user in control of the payment and can at any time choose to abort. As part of this payment process the PISP will gather and store some data, such as the identity of the user, the account from which the payment was made and the amount that is paid. This information can be said to be information that is necessary to perform the payment and the PISP so far complied with Article 66 and 67.

However, assume that there is some kind of error with the PIS service and it needs to troubleshoot/investigate. As part of that troubleshooting/investigation the PISP may want to review transaction history for a number of users to understand how severe the error is and detect the root cause of the error. Based on our understanding of paragraph 22, especially the interpretation that the compatibility test of Article 6(4) of the GDPR cannot result in a legal basis for any other processing, the PISP would not be able to perform such troubleshooting/ investigation since it would not be processing for the payment service that is requested, no consent for troubleshooting/investigation has been obtained (which is effectively not possible at the time of troubleshooting/investigation since it may involve a review of a large number of transactions) and there are no legal basis provided by Union or Member State law mandating troubleshooting/investigation. Whereas, such further processing for the purpose of troubleshooting/investigation may be lawful in line with the compatibility test of Article 6(4) of the GDPR and in light of Article 5(1)(b) and recital 50 of the GDPR.

Hence, our suggestion is that it in the Guidelines is clarified that as long as a PISP or AISP at the time of gathering and later processing of the personal data complies with GDPR, such processing of personal data is indeed lawful. This conclusion is not contradicted by Article 66 and 67 which should be understood as requirements from a PSD2 perspective only.

Article 92 - explicit consent

EPIF shares the EDPB's conclusion in paragraph 43 in the Guidelines, regarding that explicit consent under the PSD2 is a different concept as compared to (explicit) consent under the GDPR and that explicit consent in line with Article 94(2) of the PSD2 is an additional requirement of a contractual nature. Consequently, which also follows from paragraph 35 in the Guidelines, the legal basis for the processing of personal data for the provision of payment services is, in principle, Article 6(1)(b) of the GDPR.

We would like to point out that the PSD2 does not stipulate any requirements as to how a payment service provider shall acquire explicit consent from a payment service user, contrary to what is set out for a valid consent in line with Article 7 of the GDPR. Furthermore, since the legal basis for processing of personal data for the provision of payment services in principle is Article 6(1)(b) of the GDPR, there are also no requirements as to how said legal basis is to be applied by payment service providers in the context of payment services in light of Article 94(2) of the PSD2, provided that users of payment services are made fully aware of the specific categories of personal data that will be processed and the specific (payment service) purpose for which the users' personal data will be processed.

That said, in our view, it is up to each payment service provider to choose, at their own discretion, how to implement appropriate solutions to be able to comply with Article 94(2) of the PSD2, taking into account inter alia the unique characteristics of the provided payment service.

This discretion is rather necessary for payment service providers to be able to comply with the regulations in practice. We believe that the Guidelines would benefit by acknowledging this fact.

Needless to say, payment service providers of course despite such a statement have a – separate – obligation to comply with the requirements set out in the GDPR for processing of personal data, in particular as regards e.g. the principles (Article 5), legal basis (Article 6) and providing information (Article 13) in a transparent way (Article 12).

Processing of special categories of personal data under the PSD2

The GDPR article 9 conditions should only apply when a payment service provider is intended to process special categories of personal data for the purpose of essentially inferring the information they provide (but not when the processing of those data is incidental).

On processing it needs to be reminded that payment service providers are not collecting and processing data with the intent to identify health condition or political opinion. Such information can be considered as special category of data only indirectly and not systematically (e.g. a transaction at a pharmacist can be made because of a health condition or just to buy tooth path or baby formula…). As such, payment service providers shall not be considered as processing special category of data as long as the personal data involved is solely processed in order to provide the payment service.

In this respect, the suggestion made in paragraph 52 (*"In this regard, it is recommended to at least map out and categorize precisely what kind of personal data will be processed. Most probably, a Data Protection Impact Assessment (DPIA) will be required in accordance with article 35 GDPR, which will help in this mapping exercise."*) does not seem achievable. The data would have to be interpreted by the PSP with a high risk of error and this mapping would be meaningless.

If the transactional data collected by the PSPs is interpreted by the EDPB as special category of data, it is critical to clarify that this processing meets the criteria of substantial public interest (see paragraph 55). The criteria of substantial public interest, as an adequate GDPR legal ground, is unlikely to be met when transactional data are processed for purposes other than payment services themselves (e.g. marketing ones), so the only sensible interpretation would be only urging to consider the GDPR article 9 conditions apply exclusively when the purpose of processing those data is to essentially extract and use the information that could reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

As a matter of fact, processing transactional data is inherent to payment services, restricting the processing of such data for certain category of goods or services would contradict the aim of PSD2 and the single European payment area. Relying on choice would be misleading for the data subject (PSPs are not processing the information in order to identify health condition, political opinion…). This also could lead to unintended consequence. For instance, if the data subject was objecting to the processing of these categories of data, the PSP couldn't facilitate payment to certain beneficiaries (hospital, churches…)."